REMARKS

This Amendment is in response to the Office Action of November 30, 2007 in which claims 1-24 were finally rejected. Entry and reconsideration of the amended claims is respectfully requested. These changes are made because of the Examiner's contradictory and inconsistent interpretation of the supposed session and whitening keys of the reference (discussed with respect to the first and second keys of claims 1 and 2 below) and could not have been made earlier because applicant could not have anticipated such lack of full explanation and contradictory and inconsistent interpretations. They are also made because of the Examiner not showing where exactly is the server (added in the last amendment and discussed below) in the *Cassagnol et al* reference. No further search or substantial consideration is necessary.

With respect to claim 1, the Examiner argues that the step that applicant primarily relied on, i.e. "receiving, at said secure environment, via a secure channel, from a server device, a first key for decrypting said encrypted application" is known from paragraph [0011].

As regards paragraph [0011] a "first key" as such is not discussed in the reference nor is a server. If such a first key were present, for the sake of argument, it might be identified as a "session key" for use by the cipherer 20 in decrypting encrypted information. But a server cannot be seen nor can there be found a server providing a first key to a terminal over a secure channel.

Having referred to paragraph [0011], with respect to claim 1, the Examiner refers to paragraph [0025] when it comes to the step of decrypting the application with "the" first key.

In contrast, the "key" in paragraph [0025] must be identified a "whitening" key for masking the re-encryption of the information before it is sent out of the secure environment of the ASIC apparatus 10 to the external memory 24. It is clear that the "whitening" key is not the same as a first "session key" that might be used by the cipherer to decrypt encrypted information in the first place or to re-encrypt the information after use and possible modification in the secure environment. Rather, *Cassagnol et al* shows whitening keys being used in an ASIC to mask (from hackers) modifications made to re-encrypted information prior to being sent outside the secure environment of the ASIC.

In other words, the second (whitening key) is not used *per se* to re-encrypt the information but to mask modifications made to the underlying information that might be susceptible to attack by a hacker despite being subjected to re-encryption before leaving the secure environment.

With regard to claim 2, in contradiction to the interpretation of the *Cassagnol et al* disclosure with respect to claim 1, the Examiner again refers to paragraphs [0011]-[0012] for the first key but then refers to paragraph [0058] for showing a second key used for encrypting the first key. But paragraph [0058] shows a way to save memory in the secure environment by storing the whitening keys themselves outside the secure environment along with the information re-encrypted in parts using an encryption key such as the first key with whitening. Consequently, the first key is not itself encrypted using the whitening key. Rather, the whitening key is the key that is encrypted by the cipherer 20 along with the re-encrypted information.

This contradiction and inconsistency in interpretation of exactly what the *Cassagnol et al* reference shows in regard to the first and second keys make it difficult to accept that the claims, even before the above amendment, were anticipated by the *Cassagnol et al* reference.

Furthermore, considering the independent claims pending after the last amendment, in conjunction with applicant's remarks in the last response, it was implicitly but not explicitly defined that the "first key" is generated externally of the terminal device. By the above amendment, the claims are even more clearly directed to the first key being generated outside of the terminal device. The origination of the first key in this way may seem to be a minor difference to the Examiner, but it does actually make a significant difference, because a third party, such as for instance an application provider, will be able to handle the key management, and the same key can be later used to decrypt other applications from the same provider. This allows the provider to avoid the setup steps described in the specification. The Examiner is requested to consider this difference and is respectfully requested to enter the above amendment. The applicant has also made some additional amendments to remove preambles, to correct inadvertent errors in claims 22-24, and to make the claims cover a single actor rather than the former system-oriented claims requiring two actors to infringe.

The objections and rejections of the Final Action of November 30, 2007, having been obviated by amendment or shown to be inapplicable, withdrawal thereof is requested and passage of claims 1-24 to issue is earnestly solicited.

Respectfully submitted,

/Francis J. Maguire/

Francis J. Maguire
Registration No. 31,391
Attorney for the Applicant

FJM/mo
Ware, Fressola, Van Der Sluys & Adolphson LLP
755 Main Street, P.O. Box 224
Monroe, CT 06468
(203) 261-1234